Nota de l'assessoria jurídica sobre el reglament europeu de protecció de dades personals en l'exercici de la professió

El dia 25 de maig de 2018 entra en vigor el Reglament 2016/679 del Parlament Europeu i del Consell de 27 de abril de 2016, relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació de les mateixes.

L'objectiu del Reglament de Protecció de Dades Personals (RPDP) és unificar la normativa dels diferents Estats Membres, adaptar-se a l'evolució tecnològica i a la globalització, i augmentar el nivell de protecció de les dades de les persones físiques.

Ens podem preguntar si el RGPD és d'aplicació a l'exercici de la nostra professió i la resposta és clarament afirmativa: si tractem amb dades personals, desenvolupem una activitat econòmica i ho fem dintre del territori de la Unió Europea, estem obligats a complir amb les disposicions del Reglament.

A diferència de l'anterior normativa (Directiva de l'any 1995 i la Llei Orgànica de Protecció de Dades de 13 de desembre de 1999), que era un sistema de compliment més formal, el nou Reglament presenta una mentalitat més europea i es basa en una responsabilitat proactiva (*accountability*), en el sentit que obliga a cada professional o empresari a fer un anàlisi del risc de les dades personals que tracta i a valorar i decidir quines mesures de seguretat adopta per garantir la protecció de les dades.

Les obligacions principals que ens imposa el Reglament són:

a) Fer una **anàlisi i justificació que determini perquè es tracten les dades personals**: s'ha de valorar si el tractament és necessari per al compliment d'una obligació legal (per exemple, quan l'Agència Tributària o una autoritat judicial ens demana informació d'un client), per al compliment d'un contracte o per satisfer interessos legítims. Si no, és necessari obtenir el consentiment de l'interessat per poder tractar les seves dades.

b) El **consentiment de l'interessat** ha de ser demostrable, exprés, revocable, informat i ha de recaure per totes les finalitats per les quals es tracten les dades. Per tant, s'han de revisar els contractes que utilitzem i incorporar clàusules que incorporin aquest consentiment.

c) No es poden recollir més dades que les estrictament necessàries per la **finalitat** que es tracti ni guardar-les més temps del necessari.

d) Quan es **cedeixen dades personals a un tercer**, com a una gestoria per a que ens tramiti la presentació d'impostos, hem de procurar que ens signi un contracte on es comprometi a complir amb tota la normativa d'aplicació.

e) Després d'avaluar els riscos, s'han d'**adoptar les mesures proporcionals i apropiades** per a garantir un nivell de seguretat adequat al risc. Aquestes mesures, tant de tipus tècnic, com organitzatiu, han de garantir la confidencialitat, la integritat i la disponibilitat permanent dels sistemes, així com la capacitat de restaurar la disponibilitat de les dades.

f) Quan es produeix una violació de la seguretat de les dades personals, s'ha de **notificar a l'autoritat de control en un termini màxim de 72 hores**, proposant quines mesures s'adoptaran per mitigar els efectes d'aquesta violació. També s'ha d'informar als interessats dels quals tenim dades.

g) Els contractes han d'incloure clàusules informant dels **drets que tenen els interessats** i també s'han de preveure els mecanismes perquè els puguin exercitar: dret d'accés, de rectificació, de cancel·lació, d'oposició, de limitació del tractament, de portabilitat o a traslladar les dades d'un proveïdor de serveis sense necessitat que siguin transmesos prèviament a l'interessat, de revocació i a rebre comunicació de violacions de seguretat que comportin un risc.

En tot cas, entenc imprescindible **documentar totes les actuacions** que es realitzin per poder acreditar la diligència en el compliment del RGPD, ja que les sancions per infraccions es preveuen molt elevades.

Per altra banda, amb el RPDP s'elimina certa burocràcia i, en aquest sentit, desapareix l'obligació d'inscriure els fitxers de dades personals a l'Agencia Española de Protección de Datos.

Així mateix, pels professionals que no tractin dades personals a gran escala, com seria el nostre cas, no hi ha obligació de designar un delegat de protecció de dades.

Per poder adaptar-nos a aquesta nova normativa, l'Agencia Española de Protección de Datos i l'Autoritat Catalana de Protecció de Dades han publicat a les seves respectives pàgines web diverses guies i llistats que ens poden ser d'utilitat, destacant el **programa "FACILITA"** de l'Agencia Española, el qual, després de contestar un formulari online, crea un document amb una guia personalitzada per les necessitats de cadascú amb models per incloure als contractes, un registre d'activitats i un llistat de les mesures de seguretat mínimes que s'haurien d'adoptar.

Meritxell Escudé Bru
Maig 2018